بسم الله الرحمن الرحيم و الصلاة و السلام علي المبعوث رحمة للعالمين , أما بعد ,

فيسعدنا أن نقدم إلي الإخوة في أجناد مصر , هذه المسودة التي توضح كيفية إنشاء قناة إتصال آمنة بإذن الله لتبادل الرسائل الالكترونية, هذه المسودة ستحتوي فقط علي الشرح النظري للنظام و مكوناته, وسيُرفق مع هذه المسودة إصدارين مدتهما تقريبا 35 دقيقة نوضح فيهم الجزء العملي لتنصيب و إستخدام هذا النظام الآمن.

ونرجو الله تعالي أن يتقبل أعمالنا و أن يجّنب أقلامنا الزلل و ألا يؤتي المسلمون من قبلنا

القسم التقني
فريق أمن المعلومات

المقدمة

لن نعيد سرد ما تم سرده من قبل عن أهمية أمن المعلومات و خطورة هذا الثغر بشدة خاصة في ظل التطور الهائل الحاصل في مجال الاتصالات و الشبكات و الذي يتبعه تطور هائل في القدرة علي التجسس و استقاء المعلومات و تصنيفها بشكل تلقائي/ذاتي و رأينا كلنا ما سُرب من جهاز الامن القومي الامريكي الشهور الماضية و تنسيقه مع الشركات العالمية لتسريب المكالمات و المحادثات الشخصيه لمستخدميهم و رأينا التقارير المنشورة عن كيفية إستغلالهم المنتديات الجهادية لرصد من قد يمثل تهديد مُحتمل لهم.
لن نتحدث كثيرا , فلسنا أهل البلاغة و البيان , فهذه المسودة ستخرج من القسم التقني , إليكم فورا لتسريع إقامة قناة الإتصال ولن تمر بمسئولي الإعلام لكي يعيدوا صياغتها و يصمموا التصميمات الملائمة الي آخر هذه الامور, و نحسب أنكم لستم بحاجه الي تنميق العبارات و إختيار الصور الملائمة , فلستم من العوام الذين نسعي الي إثارة عاطفتهم و إنارة عقولهم.

عودة إلي الحديث عن نظام الإتصال الآمن, لا يسعنا شرح خصائص النظام و مكوناته بدون التطرق الي الحديث عن المخاطر الحالية الموجودة في نظم الاتصالات و الانترنت خاصة في ظل هذا التنسيق المخابراتي العالمي لتحليل كل شارة و واردة عبر الانترنت و تصنيفها و تخزينها
و لتحديد المخاطر سنذكر ثلاثة أمثلة عملية و نذكر فيهم المخاطر:

أول مثال: الـ Whatsapp الذي كان يتم استخدامه بكثرة بين المجاهدين, هذا البرنامج يقوم بنقل الرسائل "بدون أي تشفير" بالاضافة الي ان مبرمج البرنامج يهودي صهيوني و البرنامج "غير مفتوح المصدر". ماذا يعني هذا الكلام ؟ اولا: البرنامج ينقل الرسائل بطريقة غير مشفرة, هذا يعني ان اي موجه بيانات ستمر من عليه هذه الرسائل سيستطيع بكل سهولة رؤيتها و تحليلها و تحديد هوية راسلها, و هذا ينقلنا إلي سؤال آخر, علي من تمر البيانات؟ اولا و بلا شك , مزود الخدمة الذي تتصل بالانترنت من خلالة, اذا تكلمنا عن داخل كل بلد سوف تجد ان الحكومة تملك البنية التحتية الكاملة لشبكة الاتصالات و هذا يسمح لها برؤية البيانات و التحكم فيها بل و تقوم بتحليل كل انواع البيانات و تقوم بعمل جدولة تلقائية للبيانات و يمكن ان تربط كل البيانات ببعض و تربط البيانات باسماء الاشخاص بدون تدخل بشر و قد نشر موقع مصراوي عن صفقة حدثت لوزارة الداخلية المصرية المجرمة قامت بشراء هذه الاجهزة و سخرت الناس وقتها من ذلك مع انه حقيقي و يمكن ان ترجع للخبر حتي تقرأ كتيب عرض البيع الذي نشرة مصراوي و ما فيه من تفصيلات تقنية حتي تفهم اكثر من ذلك

لهذا يجب ان تفهم ان صندوق الخاص الذي في حسابك يمكن ان يتم التجسس عليه من قبل اجهزة الامن المختلفة خاصة انني سمعت ان نظام الشات الذي تستخدمة الفيس بوك ليس بمشفر اصلا و هذه كارثة هذا يعني انه حتي اذا توصلت بشبكتك ان اري كل البيانات .التي ترسلها عبر الشات

هل مزود الخدمة و امن الدولة فقط؟ لا بل شركة Whatsapp نفسها و التي تمر الرسائل عبرها تستطيع رؤية رسائلك و تحليلها و تخزينها(الشركة الصهيوأمريكية) و في النهاية , مزود الخدمة للطرف الآخر.
ماذا يعني كون البرنامج "غير مفتوح المصدر" ؟ ببساطة شديدة , التروجان او كما يُطلق عليه فيروس , هذه البرمجيات الخبيثة التي تستخدم للتجسس علي الاجهزة و الحواسيب , مماذا تتكون ؟ ليست إلا كود صغير يستخدم لتنفيذ اوامر خبيثة , ما علاقة هذا بالـ Whatsapp ؟ نحن لا نري الكود المصدري لبرنامج Whatsapp, نحن لا نستطيع التأكد أنه لا يحتوي علي أسطر برمجية خبيثه تستخدم لسرقه بياناتنا و اماكن تواجدنا و صورنا, و بالتالي يصبح برنامج الواتسآب في نظرنا, برنامج ملغم في حد ذاته.

ثاني مثال: لتوضيح نوعية أخري من المخاطر, تصوّر أنه قام أحد الاخوة بالدخول الي أحد المواقع الجهادية كشموخ الإسلام او الفداء الإسلامي, و لم يكن يستخدم احد برامج التخفي ك تور مثلا, سيتم "تتبعه" و تحديد الـ IP الخاص به و عن طريق مزود الخدمة الخاص به, سيتم تحديد عنوانه و شخصيته بالضبط.

المثال الأخير: تصوّر أن احد الاخوة قام بالدخول إلي أحد المواقع الجهادية بإستخدام تور و قام بالدخول الي قسم التصميمات و قام بتنزيل فلتر للفوتوشوب ليقوم بإستخدامه في تصميماته, وكان هذا "الملف ملغوم" بـ Key Logger (مسجّل مفاتيح – برمجية خبيثة لتسجيل كل ما تقوم بالضغط عليه علي لوحة المفاتيح) مثلا, هذا الاخ سيتم معرفة بريده الالكتروني بكلمة السر الخاصة به, حساب الفيسبوك الخاص به, كل ما يكتبه علي جهازه سيصبح مُسجّل و مرصود, ناهيك بالطبع عن ان سيتم معرفة الـ IP الحقيقي الخاص به.

هذه الثلاث أمثلة أوضحت لنا عدة مخاطر, ملخصها:
1–نقل البيانات بدون تشفير.
2–برمجيات غير مفتوحة المصدر.
3–التتبع.
4–الملفات الملغومه.

ما سيقوم به نظامنا للإتصال الآمن سيكون كالآتي:
1–غير قابل للتتبع ––باستخدام––> Tor Network بالاضافة الي استخدام Tor Hidden services
2–إستخدام تشفير من الطرف الي الطرف ––بإستخدام––> خوارزمية/بروتوكل PGP

3-غير قابل لحفظ الملفات الملغومة --بإستخدام--> نظام Tails الآمن

و إليكم التفصيل لشرح كل جزئية سنقوم بإستخدامها:

1- شبكة التور Tor Network

الحمدلله, أغلب الإخوة يعرفون و يستخدمون بالفعل نظام و متصفح تور للتخفي, ولكني سأقوم بشرح جزئية صغيره فيه ستفيدني في شرح بقية الأجزاء.

ما هي شبكة تور ؟

إن كان في مقدورنا وصف شبكة الإنترنت العادي , بشوارع المدينة و طرقاتها الواضحة الظاهرة للعيان و التي يسير عبرها أغلب او كل البشر تقريبا. ف شبكة التور هي شبكة المجاري الموجودة أسفل هذه الطرقات. هذا بالضبط هو أفضل وصف لشبكة التور.

وكما أن لشبكة المجاري بالوعات للنزول و الخروج منها, كذلك شبكة التور لها نقاط دخول و نقاط خروج.

نأخذ مثال أنك أردت فتح موقع شموخ الإسلام مثلا.

في حالة الإنترنت العادي(شوارع المدينة) سيقوم جهازك بتحديد عنوان الخادم الخاص بالموقع (server) و يقوم بإرسال طلب فتحه, يذهب طلبك هذا عبر مزود الخدمة الخاص بك (الذي تصل من خلاله للانترنت و لا سبيل لك الا بالمرور عليه في الذهاب و الإياب)

جهازك --> مزود الخدمة --> خادم شموخ الإسلام

في حالة متصفح التور

سيقوم البرنامج/المتصفح بتحديد احدي نقاط الدخول لك لتقوم باستخدامها بشكل عشوائي, فيخرج طلب فتح الموقع من عندك الي نقطة الدخول (مارا بالطبع بمزود الخدمة -لا مناص من ذلك-)

جهازك --> مزود الخدمة --> نقطة الدخول (فتحة البالوعة)

ثم تقوم نقطة الدخول الي إرسال طلبك الي نقطة وسيطة داخل شبكة التور نفسها (داخل المجاري) , ثم تقوم النقطة الوسيطة بتمرير طلبك الي نقطة الخروج داخل شبكة التور , و في النهاية تقوم نقطة الخروج بإيصال طلبك الي خادم شموخ الإسلام نفسه, فيمر طلبك بهذه المراحل الاتية.

جهازك --> مزود الخدمة --> نقطة الدخول --> نقطة وسيطة --> نقطة الخروج --> خادم شموخ الإسلام

شـــارع -->شبـــــــــــــــــــــــــكـــــــــــــة المجـــــــــــاري --> شـــارع

إن أفترضنا و هو إفتراض صحيح , ان كل نقطة من هذه النقاط - سواء كان التصفح العادي او تور - تستطيع معرفة النقطة التي تليها و التي تسبقها, فسنستطيع فهم كيف يحمينا متصفح التور, ففي حالة التصفح العادي , مزود الخدمة , يعرف عنوان جهازي و يعرف بأني ذهبت الي موقع شموخ الإسلام (أمن الدولة سيطرق بابك قريبا :)) في حالة متصفح التور , مزود الخدمة لا يستطيع معرفة وجهتي , هو فقط استطاع معرفة أني اقوم بإستخدام تور و لكنه لم يستطع ان يحدد إلي أي المواقع ذهبت.

هذا عن مزود الخدمة, اما مراقبي الانترنت عامة كوكالة الامن القومي الامريكية, فتستطيع مراقبة كل ما هو مار عبر الشارع و لكن بمجرد نزولي الي شبكة المجاري اسفل الشارع, فهنا يبدأ المرح الحقيقي و التحدي الحقيقي لهم, فهم يستطيعون رؤية الالاف

الطلبات الداخلة الي شبكة المجاري و يقابلها الالاف اخري خارجة , و لكن كيف يستطيعون تحديد أي طلب من الالاف الطلبات الداخلة هو من قام بطلب الوصول الي موقع شموخ الإسلام؟ هنا يبزغ أهمية علم الإحصاء و المعلن حتي الآن إنه لم يستطع احد الوصول الي كسر الخوارزمية المستخدمة في شبكة التور و قد قامت المخابرات الروسية منذ شهرين تقريبا بإعلان مكافئة 5 مليون روبل لمن يستطيع كسر هذه الخوارزمية.

عامة, ما أريد التأكيد عليه هنا, هو تذكر المثال الذي ذكرناه , شبكة التور هي شبكة المجاري اسفل المدينة و التي يصعب مراقبتها بشدة و لا يمكن رؤية كيف يتحرك فيها الناس.

ملحوظة أخيرة قبل الانتقال الي نقطة أخري : القول بأن وكالة الامن القومي الامريكية تستطيع رؤية الالاف الطلبات الداخلة و الخارجه من المجاري/شبكة–التور , هذا بإفتراض أن كل نقاط الدخول و الخروج مخترقة من او تُدار بواسطة جهاز الامن القومي الامريكي, و هو إفتراض صعب ولكنه ليس مستحيل وهم يسعون إليه.

2-التشفير (خصوصية جيدة جدا Pretty Good Privacy PGP)

إذا كان الإخوة العسكريون يقولون أن العبوات و المفخخات أنجع, فيسعنا القول بالمثل في عالم أمن المعلومات: التشفير أنكي و أنجع.
و سبحان الله, منذ بضعة أيام خرج علينا علج البريطانيين ديفيد كاميرون في احد المؤتمرات بعد غزوة شارلي إبيدو المباركة ليعلن صراحة أنه إن تم إنتخابه لولاية جديدة سيعمل علي تمرير قانون لحظر ومنع كل برامج الاتصال المشفر لعدم قدرة الحكومات علي مراقبتها و متابعة ما يكتب فيه, أعلنها صراحة.
ومن قبله نشرت صحيفة دير شبيجل الالمانية, تقرير مسرب من وكالة الامن القومي الامريكية عام 2012, يتحدث عن ان من أكبر التحديات التي يواجهونها هي خوارزميات التشفير.
و هناك اخبار كثيرة مُعلنة في الغرب لجرائم استطاع فاعلوها الهرب من العقاب لعدم قدرة الاجهزة الامنية من فك الملفات المشفرة.
مما أدي إلي أن أصدرت بريطانيا قانون رسمي عام 2009 تقريبا, يقول بمعاقبة من يرفض ان يعطي الحكومة كلمات السر و مفاتيح التشفير الخاصة به إذا طلبتهم الحكومة منه.

هذا عن التشفير عامة, ماذا تكون هذه الـ PGP المكتوبة في العنوان ؟
الـ PGP هي خوارزمية رياضية ابتكرها أحد علماء الرياضيات عام 1991 و ظلت تُطور حتي يومنا هذا, و حتي الآن لم يُعلن أنه إستطاع احد كسر هذه الخوارزمية.

لفهم نظرية عمل و نقاط قوة الـ PGP يجب علينا فهم ثلاث مصطلحات.

اولا: التشفير من الطرف الي الطرف End to End Encryption : و هو مصطلح يشير الي أن عملية التشفير تتم علي جهاز المُرسل نفسه قبل ان يتم إرسالها, و لا يتم فك تشفيرها إلا بواسطة المستقبل و لا يمكن لأي طرف بينهما فك تشفيرها او معرفة محتواها.

ثانيا: التشفير التماثلي: و هو أحد انواع التشفير و فيه يتم تشفير الرسالة الخاصة بك بـ "مفتاح" و لكي يتم فك تشفيرها يجب ان يُستخدم نفس "المفتاح" و بالتالي فـ المُرسل و المُستقبل يجب ان يتشاركا نفس المفتاح, و اي أحد يملك هذا المفتاح يستطيع فتح الرسائل و معرفة محتواها.

ثالثا: التشفير غير التماثلي: وهو نوع آخر من أنواع التشفير و فيه, يكون لكل مرسل و كل مستقبل مفتاحين منفصلين ولكن تربطهم علاقة رياضية معينة, مفتاح عام Public Key و مفتاح خاص Private Key.

و من خصائصه, إن قمت بتشفير الرسالة بـ المفتاح العام لشخص ما, فإنه لن يتم فك تشفيرها إلا بواسطة المفتاح الخاص المرتبط بهذا المفتاح العام,, حتي المفتاح العام الذي قمت بتشفيرها به , لن أستطيع فك تشفيرها بواسطته.

ولذلك سُمي احد هؤلاء المفاتيح بالمفتاح العام, لأنه لا يتم إخفائه بل بالعكس يتم نشره و وضعه علي الملأ, فمن يريد مراسلتك, سيكتب الرسالة ثم سيشفرها بواسطة مفتاحك العام , وبالتالي لن يستطيع أي احد فك تشفيرها الا من يملك المفتاح الخاص المقابل لمفتاحك العام, وبطبيعة الحال سيكون هذا الشخص هو أنت.

لكي نوضح هذا الامر أكثر, سنضرب مثال صغير , نفترض وجود شخصين أحدهم يُدعي الاجناد و الاخر يُدعي الانصار, لكل واحدا منهما مفتاحين خاص وعام.
فيوجد أربع مفاتيح :

المفتاح العام للأجناد
المفتاح الخاص للأجناد
المفتاح العام للأنصار
المفتاح الخاص للأنصار

إذا أراد الاجناد ان يرسل رسالة مشفرة إلي الانصار, فسيقوم بكتابة الرسالة , ثم يقوم بتشفيرها بواسطة المفتاح العام للأنصار, عند إستقبال الأنصار لهذه الرسالة المشفرة سيقوم بفك تشفيرها بواسطة المفتاخ الخاص للانصار.
و العكس بالعكس , إذا أراد الانصار ان يرد علي الاجناد , فسيقوم بكتابة رده و من ثم تشفيره بواسطة المفتاح العام للاجناد , وعند استقبال الاجناد له سيقوم بفك تشفيره بواسطه المفتاح الخاص للاجناد.

حسنا, حتي الأن, بواسطة التشفير غير التماثلي نستطيع ان نضمن أنه لن يستطع أحد فك تشفير الرسالة إلا الشخص المُرسل إليه.

بقي شئ أخير, كيف يستطيع المُرسل إليه أن يضمن أن المرسل هو كما يدعي بالفعل ؟ بمعني آخر, الشخص المُسمي الأجناد, إذا جائتهم رسالة مُشفرة بمفتاحهم العام, و المرسل يدعي أنه الشخص المدعو الأنصار, كيف يسعهم التأكد من هويته ؟؟؟

في حياتنا العادية, و تبادل المراسلات و الخطابات الورقية, يقوم مُرسل الخطاب, بكتابة توقيعه في آخر الخطاب, لكي يثبت هويته للمُرسل إليه.

هذا بالضبط ما سعوا لفعله, فأخرجوا مصطلح جديد بجانب مصطلح التشفير و هو مصطلح التوقيع Signing

كيف يتم التوقيع ؟
قلنا من قبل أن كل شخص له مفتاحان, عام و خاص, العام منشور علي الملأ و الكل يعرفه, الخاص لا أحد يعرفه إلا صاحب المفتاح.
وقلنا أيضا, أن الرسالة المُشفرة بالمفتاح العام لا يتم فك تشفيرها إلا بالمفتاح الخاص المرتبط بهذا المفتاح العام.
سنزيد قولنا هنا و نقول أنه, إن شُفرت الرسالة بالمفتاح الخاص, لا يتم فك تشفيرها إلا بالمفتاح العام !!

فالقاعدة العامة هنا : ما تم تشفيره بأحد المفاتيح, يتم فك تشفيره بالمفتاح الآخر.

كيف نستغل هذه القاعدة لتحقيق مبدأ التوقيع ؟
يقوم المُرسِل بتشفير رسالته بالمفتاح العام للمُرسل إليه, كما قلنا من قبل, ولكنه يضيف في آخر الرسالة جزء آخر , يتم تشفيره بواسطة المفتاح الخاص للمُرسِل.

فإذا وصلت الرسالة إلي الطرف الآخر, سيفك الجزء العلوي بشكل طبيعي بالمفتاح الخاص للمُرسَل إليه, و سيقوم أيضا بالتحقق من الجزء السفلي من الرسالة عن طريق فك تشفيرها بواسطة المفتاح العام للمُرسِل, فإن نجح في فك تشفيره, اذا فهذا الشخص هو فعلا صاحب المفتاح العام. و إن لم ينجح في فك تشفيرها, فليس هو كما يدعي.

ملحوظة : عملية التشفير تسمي Encryption و فك التشفير Decrypyion
عملية التوقيع تسمي Signing و عملية التحقق من التوقيع تسمي Verifying

و هكذا نكون أنهينا الحديث عن مصطلحات التشفير.
و بالتأكيد لا أحتاج أن أقول ان خوارزمية PGP هي احدي تطبيقات التشفير من الطرف إلي الطرف و يستخدم نظرية التشفير غير التماثلي.

و كما قلنا من قبل الخوارزمية الرياضية للـ PGP لم يُعلن حتي الان إنه تم إختراقها او كسرها, ولذا فهذا النوع من التشفير آمن في حد ذاته ولكن هل هو آمن بشكل عام ؟ كيف تعاملت المخابرات العالمية معه ؟ كيف إستطاعوا تخطيه؟ ما هي الثغرة التي إستطاعوا إستغلالها لتخطيه؟

الثغرة الأساسية التي يستغلونها هي جهاز الحاسوب نفسه, هو يعلم إنه لن يستطيع فتح الرسالة بدون المفتاح الخاص للمُرسل إليه , فأصبح سعيه الحثيث لتخطي هذا هو إما بإختراق جهاز المُرسِل و وضع فيه Key-Logger (برمجية خبيثة تقوم بتسجيل كل ما يتم كتابته علي لوحة المفاتيح) فأصبح يستطيع قراءة الرسالة من قبل أن يتم تشفيرها أصلا, او يقوم بإختراق جهاز المُرسل إليه و

يقوم بسرقة المفتاح الخاص المخزن عليه.

هذه هي الثغرة الأساسية , السؤال ما مدي نجاحهم في استغلال هذه الثغرة؟ المنشور و المُسرب يشير الي أنهم يدركون ما يفعلون جيدا, إقرأ هذا التقرير المنشور في مجلة "زا ريجيستر" البريطانية لكي تتخيل إلي ماذا وصلوا
http://www.theregister.co.uk/2014/03/12/snowden_docs_show_nsas_malware_turbine_can_pump_out_millions_of_malware_attacks/?page=1

و خطورة هذه الثغرة تتعاظم بعد معرفتنا أنهم ليسوا بحاجه إلي إرسال ملفات ملغومة إلي ضحاياهم أصلا بل وليسوا بحاجه إلي إرسال مسجل مفاتيح Keylogger, فالتقارير التي سربها إدوارد سنودن توضح انه يجري تنسيق كبير بين وكالة الامن القومي الامريكية و شركة مايكروسوفت, مثلا نظام ويندوز التي تنتجه شركة مايكروسوفت نظام مغلق المصدر , الكود المصدري الخاص به غير منشور ولا يمكن لخبراء امن المعلومات الإطلاع عليه للتأكد من خلوه من ثغرات او أسطر برمجية خبيثة, بل و لا يمر أسبوع إلا وتخرج علينا شركة مايكروسوفت لتعلن عن وجود ثغرة جديدة تم اكتشافها و تعلن عن سدها, فإن كان هذا هو المعلن, فكم ثغرة لم يُعلن عنها و جاري استغلالها حاليا !!
منذ عدة شهور تم إكتشاف ثغرة خطيرة في بروتوكل التشفير SSL, الثغرة موجودة منذ ثلاث سنوات و لم يكتشفها أحد, و تناثرت عدة إتهامات موجهة الي وكالة الامن القومي الامريكية بأنها كانت تعلم بخصوص الثغرة ولم تعلن عنها و ظلت عامان تستغلها.

ما الحل ؟ كيف نستطيع تأمين أنفسنا؟ كيف نستطيع تأمين مفاتيح التأمين الخاصة بنا من السرقة ؟
ما نحن بصدده الآن هو الحديث عن إنشاء قناة إتصال آمنة, فلن نتطرق إلي طرق التأمين العامة حاليا لكي لا نطيل الحديث.
أفضل وسيلة لمقاومة هذه الثغرة و تأمين مفاتيح التشفير الخاصة بنا و حماية أجهزتنا من الاختراق و التلغيم بإذن الله, هو بإستخدام النظام الآمن Tails, وهذا هو النقطة الثالثة في حديثنا اليوم.

3-نظام Tails الآمن

قبل الشروع في توضيح ماهية نظام تايلز و نظرية عمله و نقاط قوته وضعفه, استهل الحديث عنه بذكر أن آخر تقرير منشور في مجلة دير شبيجل الالمانية و الذي نُشر فيه تقرير مُسرب من وكالة الامن القومي الامريكية مصنف بـ سري للغاية ومكتوب عام 2012 , يقولون فيه بأن نظام تايلز علي رأس التحديات التي يواجهونها في مراقبة الانترنت و كتبوا فيه توصيات ببذل مجهود أكبر لإختراقه.

ما هو نظام التايلز ؟
هي أحدي توزيعات اللينكس, قام بتمويل تطويرها و إنشائها الفريق الخاص بـ مشروع التور. و هي Live Operating system أي إنها لا يتم تنصيبها علي الجهاز الخاص بك, بل يتم حرقها مباشرة علي اسطوانة مدمجة او علي فلاش ديسك و يتم استخدامها مباشرة بدون تنصيب. و هذا أول مميزاتها, فهي نظام متنقل يعمل أي جهاز و غير مرتبط بنظام التشغيل الموجود علي الجهاز , فهي تعمل قبل دخولك إلي نظام التشغيل الخاص بك اصلا.
و بما إنها تعمل بإستقلالية تامة عن نظام التشغيل الخاص بك, فهي لا تتأثر إن كان نظام التشغيل الخاص بك مخترق, فحتي إن كان

جهازك مخترق, فهم لا يستطيعون مراقبة او تسجيل ما تقوم بفعله علي نظام تايلز. وهذه هي ثاني المميزات.
ثالث المميزات, هي إنها بالإعدادات الإفتراضية, لا تقوم بحفظ أي تغيير يطرأ عليها اثناء تشغيلها, فإن كنت تتصفح الانترنت من خلالها وقمت بتنزيل إصدار عليها مثلا او برنامج ما, وكان هذا الإصدار ملغم ببرمجية خبيثة, فبمجرد غلقك للجهاز و إزالتك للفلاشه , ستعود الفلاشة كما كانت من قبل و لن يتم حفظ اي تغيير.
رابع المميزات, وهي من أهم ما يميزها, أنه لا يتم الوصول إلي الانترنت من خلالها إلا عبر شبكة التور, و تقوم تلقائيا بعمل حجب لأي برنامج يحاول الوصول إلي الانترنت مباشرة بدون شبكة التور, وبالتالي فهي تضمن تأمين تام من التتبع.
خامس المميزات, تقوم تلقائيا بعمل تمويه لـ MAC address الخاص بجهازك لضمان عدم التتبع.

و الكثير من الامور الاخري و لكن هذا ما يهمنا الان لإنشاء قناة إتصال آمنة بالتكامل مع تشفير الـ PGP

هذا فقط ما سنكتبه عن نظام تايلز, وستجدون بإذن الله في الجزء العملي من الشرح, الفيديو الأول, نقوم فيه بشرح كيفية تنزيل النظام و حرقه و تغيير إعدادته لكي تلائم احتياجتنا, مدة الفيديو تقريبا 15 دقيقة.

4- الخدمات المخفية في شبكة تور Tor Hidden Services

لقد قمنا حتي الآن بشرح فكرة عمل التشفير ثم للتغلب علي الثغرة الموجودة فيه قمنا بذكر نظام تايلز الآمن, حسنا, بعد تشفير رسالتي, كيف أقوم بإرسالها ؟
هل أقوم بإرسالها في رسالة خاصة علي إحدي المنتديات الجهادية كالفداء الإسلامي او شموخ الإسلام ؟
ام أقوم بإرسالها الي حساباتكم عبر الفيسبوك ؟
ام اقوم بإرسالها عبر شئ آخر ؟؟

نعيد صياغة السؤال لكي يتضح المقصد, هل من الأفضل أن يعلم المتربصون بنا و بكم أننا نتبادل الرسائل الإلكترونية؟ ام من الافضل ألا يعلموا ؟
فيقينا, عبر الفيسبوك سيعلمون و يشاهدون الرسائل المشفرة و نحسب أنهم لن يستطيعوا فك تشفيرها بإذن الله, و لكنهم سيعلموا اننا نتبادل المعلومات.
اما علي المنتديات الجهادية, فأنا لا أعلم تحديدا التدابير الأمنية التي يتخذها الاخوة القائمون علي هذه المنتديات, ولكن ما أعلمه جيدا, أن هذه المنتديات هي الهدف الأول لقسمين علي الاقل في كل جهاز مخابرات سواء كان عربي أم غربي, فلماذا نتحدث عبره و نحن نعلم الكمية الكبيرة من الأعين المتربصة خاصة و هناك بدائل أكثر أمنا بكثير موجودة, نعم هذه البدائل تحاول أجهزة الامن حول العالم الإيقاع بها, و لكن لأسباب جنائية وصحفية وليس لأسباب تتعلق بالإرهاب و شتان الدافع, بالاضافة أن المتعارف عليه في التراسل عبر هذه البدائل هو إرسال الرسائل المشفرة, فبالتالي تبادلنا الرسائل المشفرة لن يكون ملفت للنظر ابدا بعكس المنتديات.

ما هذه البدائل ؟
فلنبدأ الحديث إذن عن خدمات تور المخفية.

سبق أن قولنا أن بفضل الله أغلب الإخوة يستخدمون بالفعل متصفح التور للتخفي, ولكن هل ما يقوم به مشروع تور هو إخفاء هوية

المتصفح فقط ام يقوم بأشياء أخري ؟!

عندما أتينا لوصف شبكة تور من قبل, قلنا أن أفضل توصيف لها لمقارنتها بالانترنت العادي , هو بوصفها شبكة المجاري الخفية عن الاعين التي تسير تحت الارض.

و قلنا أنني لكي أصل لأي موقع عبر الانترنت, يجب علي معرفة عنوانه (الايبي IP الخاص به) ثم أرسل له طلب, وشرحنا كيف يسير الطلب في حالة استخدام المتصفح العادي و في حالة متصفح التور.

وقلنا أننا في حالة متصفح التور , نقوم بالدخول الي شبكة المجاري ثم السير فيها ثم الخروج منها حتي نصل الي عنوان الموقع الذي نريد.

و قلنا أن من الثغرات التي تحاول وكالة الامن القومي الامريكية استغلالها في شبكة التور هي السيطرة علي كل مداخله و مخارجه ومن ثم تستخدم علم الاحصاء المتقدم لمحاولة الربط بين البيانات الداخله و الخارجه لتحديد هوية الاشخاص, و لكن, ماذا لو لم نخرج؟

ماذا لو قمنا بالدخول الي شبكة التور (المجاري) و إلتقينا فيها و عاد كل شخص فينا الي مكانه !! ماذا لو كان الموقع الذي أريد الذهاب إليه, موجود أسفل الارض في شبكة المجاري نفسها !!

هذا بالضبط ما يقدمه مشروع تور و غفل عنه الكثير من الإخوة عدا الإخوة في القوقاز بشبكة (Kavkaz center), مشروع تور من إحدي خصائصه أنه يسمح لك بنشر خادم (server) خاص بك و يقوم بإعطائك عنوان له لكي يستطيع الآخرون الوصول إليه, هذا العنوان ينتهي بـ .onion وليس كبقية المواقع علي الانترنت .net. com .org ....الخ, و "دوت اونيون .onion" هذه غير مدرجة في سجلات الانترنت العادي و بالتالي لا يستطيع اي احد الوصول إليها من متصفحه العادي, يجب عليه استخدام متصفح تور للوصول إليها. و ليس هذا كل ما يميزه, عندما تقوم بنشر الخادم الخاص بك, لن يتم كشف عنوانك (IP) فمشروع تور صمموا العملية بحيث تتم عملية نقل الطلب من خلال اسم الموقع نفسه مباشرة.

و نظرا لهذه الخاصية التي تقدمها شبكة تور و صعوبة تتبع مديري المواقع و الخوادم و تحديد اماكنهم, قام المجرمون و الاناركيون و تجار المخدرات و تجار السلاح, بإنشاء متاجر رسمية علي شبكة تور و شرعوا في بيع منتجاتهم بل ووصل الأمر الي شبكات بيع الاعضاء و تأجير القتلة المأجورين, باختصار كـل ما يُخالف القانون الغربي, يتم عبر هذه الشبكة و نظرا لإتساع الموضوع و ظهور مئات بل الالاف المواقع أصبح يُطلق علي هذه الشبكة بـ الانترنت السفلي Deep-Web فهي بالفعل عالم اخر من الانترنت و لكنه يجري تحت الارض.

عامة نرجع إلي حديثنا, الخادم الذي تقوم بنشره هنا, يمكنك برمجته لكي يقوم بما تشاء, فيمكنك برمجته ليعمل كـ (web server) و تضع عليه أخبارك و مقالات .... الخ ,, او يمكنك برمجته لكي يعمل كـ (Email Server) و يتم استخدامه لنقل البريد الالكتروني بين أعضائه, وهذا بالضبط ما نحتاج إليه.

أنا لا أقول بأن ننشئ خادم خاص بنا, فهذه العملية تحتاج الي متابعة دورية لضمان أمن الخادم و تطويره و لا نضمن توفر هذا الوقت و توفر الانترنت عند اشتعال الساحة هنا.

خاصة و أنه بالفعل يوجد أكثر من خادم منشور علي شبكة تور, يقدمون خدمات البريد الالكتروني بشكل مجاني و يقومون هم بإدارته.

و أذكركم, نحن لا نثق في اي شخص, ولكننا سنقوم بإرسال الرسائل بشكل مشفر, وبالتالي حتي لو قام مدير الخادم بتسريب الرسائل الالكترونية فلن يستطيع بإذن الله فك تشفيرها , و جُل ما يتم تبادله عبر هذه الخوادم تكون رسائل الكترونية مشفرة ,

وبالتالي رسائلنا ستختفي وسط مئات الرسائل الاخري ولن يظهر منها ما نفعله.

من عناوين الخوادم التي تقدم خدمة البريد الالكتروني المجاني :

Mail2tor

mail2tor3yf6k42e.onion

RuggedInbox

/http://s4bysmmsnraf7eut.onion

ويتم تسجيل الدخول عبر هذا الرابط

http://s4bysmmsnraf7eut.onion/sm

TorBox

/http://torbox3uiot6wchz.onion

و بإذن الله سنقوم في الجزء العملي الفيديو الثاني و الاخير بشرح كيفية إنشاء حساب علي mail2tor و كيفية استخدامه لإرسال الرسائل الالكترونية , و سنقوم في الفيديو ايضا بشرح كيفية إجراء عملية التشفير , مدة الفيديو تقريبا 20 دقيقة.

خاتمة

وبهذا نكون أتممنا بفضل الله شرح كل جزئية في النظام علي حدة, و لم يتبق لنا في هذه المسودة إلا توضيح كيف سنقوم بالجمع بين هذه الاجزاء لتكوين نظامنا الآمن.

ببساطة و بإختصار شديد, سنقوم بتنصيب نظام تايلز الآمن علي فلاش ديسك (فلاشه), ثم سنقوم بالدخول عليها و توليد مفاتيح تشفير خاصة بنا ثم سنقوم بإنشاء حساب بريد إلكتروني علي احدي خدمات تور المخفية.

و عندما نريد ان نتواصل سنقوم بفتح نظام تايلز ثم كتابة الرسالة وتشفيرها ثم فتح البريد الالكتروني و إرسالها عبره, هكذا ببساطة !

و أخيرا: أذكرك, الإصدارات في الجزء العملي مجتمعه مدتها تقريبا 35 دقيقة, فلا يكسلك كثرة حديثي النظري هنا, التطبيق العملي لن يأخذ أكثر من 25 دقيقة للإنتهاء من تنصيب النظام الآمن للاتصال, و تذكر أخي الحبيب, نحن نعبث مع أجهزة مخابرات عالمية — والله أعلي و أكبر— و قد أمرنا الله بالأخذ بالاسباب و التوكل عليه, فلا تتكاسل عن الاخذ باسباب التخفي, لانك ستُحاسب إن قصرت, ومن أهم النقاط التي نعتمد عليها في حربنا هي "المعلومات", فالحفاظ علي المعلومات و منع تسربها و ضمان عدم معرفة العدو بـ ما نعرفه من معلومات عنه, من أهم "أسباب" تحقق عامل المفاجأة.

فلا تجعل تكاسلك سببا في ضياع مجهود و دماء أريقت في سبيل إقامة شرع الله علي هذه الارض.

و الحمدلله رب العالمين.